# FERMAT NUMBERS $F_n = 2^{2^n} + 1$.[1]

By R. D. CARMICHAEL, University of Illinois.

## Introduction and Historical Remarks.

1. One of the most fascinating of the small separated regions of mathematics is that pertaining to the Fermat numbers[2]

$$F_n = 2^{2^n} + 1.$$

Fermat erred in the belief that every $F_n$ is a prime; though he admitted that he had no proof. He challenged other mathematicians to furnish a demonstration of this beautiful proposition, adding that such a proof would probably give the key to penetrate all the mystery of prime numbers and would release his energies so that afterwards nothing could keep him back in these matters.

A most surprising geometric connection of the numbers $F_n$ was brought to light when Gauss proved that a regular polygon of $m$ sides can be constructed by ruler and compasses if $m$ is a product of a power of 2 and distinct odd primes each of the form $F_n$ and stated that the construction is impossible when $m$ is not such a product.

2. For $n = 0, 1, 2, 3, 4$, the numbers $F_n$ are 3, 5, 17, 257, 65537, respectively. It is easy to verify directly that these are primes. No other prime $F_n$ is known as such, while for $n = 5, 6, 7, 8, 9, 11, 12, 18, 23, 36, 38, 73$ it has been shown that $F_n$ is composite. A table of all the known factors of $F_n$ is to be found in this MONTHLY, Vol. 21, 1914, p. 249, except for the required addition that $F_{73}$ has the prime factor $2^{75}.5 + 1$. (See also § 16 of the present paper.) The factors actually listed in this table are all primes. The known factorization is complete for $n = 5, 6$, but is not known to be complete for greater values of $n$.

Euler was the first to prove the falsity of Fermat's conjecture that every $F_n$ is prime; and this he did by pointing out that 641 is a factor of $F_5$. The American calculator, Zera Colburn, in his autobiography, records that while on exhibition in London, at the age of eight, he found "by the mere operation of his mind" that $F_5 = 641 \cdot 6700147$.

In view of the known facts about the factors of $F_n$, Fermat's question, whether $(2k)^{2^m} + 1$ is always a prime except when divisible by an $F_n$, is without further particular interest.

3. The principal problem so far studied in connection with the numbers $F_n$ is that of their factorization. The most elementary and obvious method for finding the factors of a given number is to test it for divisibility by primes less than its square root; but if the given number is a large prime or has only large prime

[1] Presented to the American Mathematical Society (Southwesten section), November 30, 1918.

[2] A complete history of these numbers (with full references) is given in Dickson's *History of the Theory of Numbers*, Vol. I, 1919, Chap. XV. To this the reader is directed for further references to the literature.

factors it is obvious that the labor thus involved is prohibitive. One of the earliest used improvements on this method consists in determining certain properties of the prime factors of the numbers in consideration and then testing with only those primes which have this property. Thus Euler showed that the factors of $F_n$ are of the form $2^{n+1} \cdot k + 1$ (Lucas later proved that $k$ here is even; see below). At a time when it was still unknown whether $F_6$ is prime or composite Lucas remarked that if it is prime the demonstration of this fact by aid of Euler's theorem would require a calculator the enormous period of three thousand years of painstaking toil. Lucas himself exhibited a new method (reproduced below) by which the question of the primality of $F_6$ could be determined by a single calculator in thirty hours. This method consists not in seeking the factors of $F_6$ but, strange to say, in the inverse process of ascertaining whether it is itself a factor of a number in a certain sequence.

4. Probably by far the largest calculation yet performed in connection with the theory of numbers is that by means of which Morehead and Western[1] established the composite character of $F_8$. The authors have given (*loc. cit.*) an account of their method.

It is of interest to observe the enormous bigness of the number $F_{73}$, the largest $F_n$ concerning which we know whether it is prime or composite. (It has the prime factor $2^{75}.5 + 1$.) In his *Mathematical Recreations,* 5th edition, p. 40, W. W. R. Ball remarks that if this number $F_{73}$ "were printed in full with the type and number of pages used in this book, many more volumes would be required than are contained in all the public libraries of the world." To put it differently and much more strongly we may say that if it were printed in full with the type and format of the *Encyclopædia Britannica,* eleventh edition, it would require more volumes than would be contained in 10,000,000,000,000 full sets of twenty-nine volumes each. Or if printed on ordinary 400-page octavo volumes it would make a library of more than two million volumes for each man, woman and child in the world.

5. In the present paper I have gathered together all the essential facts known about the numbers $F_n$. For the more important of these I have given (in §§ 6–11) as simple demonstrations as I could, employing methods to be found in the literature and encumbering them as little as possible to secure the end in view. I have listed (in § 13) the outstanding conjectures and have also added (in §§ 14–17) a few minor results which appear to be novel.

## Fundamental Properties of the Numbers $F_n$.

6. As far back as 1730 it was observed that no $F_n$ has a proper factor less than 100, a fact easily verified directly by the aid of congruences. More recently a considerable number of negative results of this character have been given, as, for instance, that no $F_n$ has a factor less than $10^6$ other than factors known at present; likewise there is no undiscovered factor of an $F_n$ less than $10^8$ and of the form $2^a \pm 2^x + 1$. There has also been considerable examination as to the possi-

[1] *Bull. Amer. Math. Soc.*, (2), 16 (1909), 1–6.

bility of factors of the forms

$$2^t \cdot 3 + 1, \qquad 2^t \cdot 5 + 1, \qquad 2^t \cdot 7 + 1.$$

In particular, a prime of the form $2^{2^t} \cdot 3 + 1$ cannot be a factor of a Fermat number $F_n$.[1] The smallest of the as yet known factors of each $F_n$ is actually the least factor of each such number.

Again it was noticed early that no two $F_n$ have a common factor. For, if $F_n$ and $F_m$, $m > n$, have a common prime factor $p$, then

$$2^{2^m} \equiv (2^{2^n})^{2^{m-n}} \equiv (-1)^{2^{m-n}} \equiv 1 \bmod p,$$

so that $2^{2^m} + 1$ is not divisible by $p$.

7. The first theorem about the numbers $F_n$ actually demonstrated is that of Euler to the effect that all factors of $F_n$ are of the form $2^{n+1} \cdot k + 1$. We give a proof of Lucas' extension of this theorem, namely,

*Every factor of a given number $F_n$ ($n \geqq 2$) is of the form $2^{n+2} \cdot k + 1$.*

It is sufficient to prove the theorem for a prime factor $p$ of $F_n$. Since

$$2^{2^n} \equiv -1 \bmod p$$

it is evident that $2^{n+1}$ is the exponent to which 2 belongs modulo $p$, so that $p - 1$ is divisible by $2^{n+1}$ (the result due to Euler). Now, $p$ is of the form $8t + 1$, since $n \geqq 2$. Hence 2 is a quadratic residue modulo $p$. Therefore, we have

$$2^{\frac{1}{2}(p-1)} \equiv 1 \bmod p,$$

so that $\frac{1}{2}(p - 1)$ is divisible by $2^{n+1}$, the exponent to which 2 belongs modulo $p$. From this the theorem follows at once.

By means of this theorem it is easy to establish the following proposition:

*If $f = 2^{n+2} \cdot q + 1$ is a factor of $F_n$ and $q \ngtr 9 \cdot 2^{n+2}$, then $f$ is a prime.*

For if $f$ is not prime we must have

$$f = (2^{n+2} \cdot x + 1)(2^{n+2} \cdot y + 1)$$

where $x$ and $y$ are integers greater than 2; whence we have $q > 9 \cdot 2^{n+2}$. [In this theorem 9 may be replaced by 15 if $f$ is not a square number.]

For the numbers $F_5$, $F_{12}$, $F_{23}$, $F_{36}$, $F_{38}$, $F_{73}$, the least factors to be tried (in accordance with the foregoing theorem of Lucas and the fact that no two $F_n$ have a common factor) are respectively

$$2^7 \cdot 5 + 1, \quad 2^{14} \cdot 7 + 1, \quad 2^{25} \cdot 5 + 1, \quad 2^{39} \cdot 5 + 1, \quad 2^{41} \cdot 3 + 1, \quad 2^{75} \cdot 5 + 1;$$

and in each case such number is a factor of the corresponding $F_n$. Thus of the seventeen cases in which we know at present whether the given $F_n$ is prime or composite there are five in each of which it is easily seen to be prime while in half (six in number) of the remaining cases the least number to be tried in each instance turns out to be a factor. The verification by means of congruences is

[1] *Bull. Amer. Math. Soc.*, (2), 12: 450.

easy in the first three cases and not unduly tedious in the last three cases. In view of such verification and the two theorems above it is easy to see that each of these six factors is a prime number, the last being one of twenty-four digits.

8. Since the totient $\varphi(p)$ of $p$ is less than $p - 1$ except when $p$ is a prime number, the following theorem of Lucas is an immediate consequence of the Fermat theorem $a^{\phi(m)} \equiv 1 \bmod m$:

If the congruence $a^x \equiv 1 \bmod p$ is true when $x = p - 1$ but is not true when $x$ is any proper divisor of $p - 1$, then $p$ is a prime number.

For, $a^\delta \equiv 1 \bmod p$, when $\delta$ is the greatest common divisor of $\varphi(p)$ and $p - 1$.

By means of this result it is easy to establish Pepin's theorem concerning prime numbers $F_n$:

*For $n > 1$, $F_n$ is prime if and only if it divides*

$$k^{\frac{1}{2}(F_n-1)} + 1,$$

*where $k$ is any quadratic non-residue of $F_n$, as 3 or 5 or 10.*

A test of this sort for prime numbers is remarkable in that it depends not directly on seeking factors of the number in consideration but in ascertaining whether it divides some other number.

To prove Pepin's theorem we proceed as follows: If $F_n$ is prime we have

$$k^{\frac{1}{2}(F_n-1)} \equiv -1 \bmod F_n$$

by the theory of quadratic residues. On the other hand, if the foregoing congruence is satisfied, we have

$$k^{F_n-1} \equiv 1 \bmod F_n$$

while there is no proper divisor $d$ of $F_n - 1$ for which $k^d \equiv 1 \bmod F_n$, since every such divisor is a power of 2 and a factor of $\frac{1}{2}(F_n - 1)$. Applying the theorem of Lucas at the beginning of this section we now conclude to the truth of Pepin's theorem.

To apply Pepin's test, one would take consecutively the minimum residues modulo $F_n$ of

$$k^2, k^4, k^8, \cdots, k^{2^{2^n-1}}.$$

9. Hurwitz gave the following generalization of Pepin's theorem:

Let $F_n(x)$ denote the irreducible algebraic factor of $x^n - 1$ (of degree $\varphi(n)$) which is not a factor of any $x^v - 1$ for which $v < n$. Then if there exists an integer $q$ such that $F_{p-1}(q)$ is divisible by $p$, $p$ is a prime.

When $p = 2^k + 1$ it is easy to show that $F_{p-1}(x) = x^{2^{k-1}} + 1$.

Carmichael employed the notation $F_n(\alpha, \beta)$ for $\beta^{\phi(n)} F_n(\alpha/\beta)$, where $F_n(x)$ has the meaning just defined. He gave the following generalization of the foregoing theorem of Hurwitz:

A necessary and sufficient condition that a given odd number $p$ is prime is that there exist relatively prime integers $\alpha + \beta$ and $\alpha\beta$, $\alpha$ and $\beta$ not both roots of unity, such that (the integer) $F_{p-1}(\alpha, \beta)$ is divisible by $p$.

A proof of this theorem is to be found in *Annals of Math.*, (2), 15 (1913): 66.

10. Let $\alpha + \beta$ and $\alpha\beta$ be two relatively prime integers, $\alpha$ and $\beta$ not both roots of unity, and consider the quantities

$$S_n = \alpha^n + \beta^n, \qquad D_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \alpha^{n-1} + \alpha^{n-2}\beta + \cdots + \beta^{n-1}.$$

$S_n$ and $D_n$ both represent integers, since each of them is a symmetric polynomial (with integral coefficients) in the roots $\alpha$ and $\beta$ of the equation

$$x^2 - (\alpha + \beta)x + \alpha\beta = 0$$

whose coefficients are integers. It is obvious that $D_n$ is a factor of $D_{nk}$ if $n$ and $k$ are both integers.

Let $p$ be an odd prime which is not a divisor of either $(\alpha - \beta)^2$ or $\alpha\beta$. We have

$$S_p - (\alpha + \beta) \equiv \alpha^p + \beta^p - (\alpha + \beta)^p \equiv 0 \bmod p$$

and

$$D_p - (\alpha - \beta)^{p-1} \equiv \alpha^{p-1} + \cdots + \beta^{p-1} - (\alpha - \beta)^{p-1} \equiv 0 \bmod p.$$

But it is easy to verify that

$$(\alpha + \beta)D_p - S_p = 2\alpha\beta D_{p-1}.$$

Therefore

$$(\alpha + \beta)(\alpha - \beta)^{p-1} - (\alpha + \beta) \equiv 2\alpha\beta D_{p-1} \bmod p.$$

Now $(\alpha - \beta)^2$ is an integer; hence from Fermat's theorem it follows that

$$(\alpha - \beta)^{p-1} \equiv \pm 1 \bmod p.$$

From the last two congruences we have therefore

$$D_{p-1} \equiv 0 \bmod p \qquad \text{if } (\alpha - \beta)^{p-1} \equiv 1 \bmod p,$$

$$\alpha\beta D_{p-1} \equiv -(\alpha + \beta) \bmod p \qquad \text{if } (\alpha - \beta)^{p-1} \equiv -1 \bmod p.$$

Now it is easy to verify that

$$D_{p+1} - (\alpha + \beta)D_p + \alpha\beta D_{p-1} = 0;$$

and hence we see that

$$D_{p+1} \equiv 0 \bmod p \qquad \text{if } (\alpha - \beta)^{p-1} \equiv -1 \bmod p.$$

Therefore we have the following theorem (due to Lucas):

*An odd prime $p$ which does not divide either $(\alpha - \beta)^2$ or $\alpha\beta$ is a factor of $D_{p-1}$ or of $D_{p+1}$ according as $(\alpha - \beta)^{p-1}$ is congruent to $+1$ or to $-1$* modulo $p$.

That $D_n$ and $S_n$ are both prime to $\alpha\beta$ follows at once from the readily verified relations

$$(\alpha + \beta)^n = \alpha^n + \beta^n + \alpha\beta I_1 = S_n + \alpha\beta I_1,$$

$$D_n = \alpha^{n-1} + \beta^{n-1} + \alpha\beta I_2 = S_{n-1} + \alpha\beta I_2,$$

in which $I_1$ and $I_2$ denote integers. But it is easy to show directly that

$$D_m S_n - D_n S_m = 2\alpha^n \beta^n D_{m-n}.$$

Hence a common odd prime factor $p$ of $D_m$ and $D_n$ $(m > n)$ is a factor of $D_{m-n}$; whence it follows without difficulty that $p$ is a factor of $D_v$ where $v$ is the greatest common divisor of $m$ and $n$. From this conclusion and the foregoing theorem we see that the least value $k$ of $n$ for which $D_n$ is divisible by a given prime $p$ (not dividing $(\alpha - \beta)^2$ or $\alpha\beta$) is a factor of $p - 1$ or $p + 1$ in the respective cases. Hence we have the following theorem (also due to Lucas):

*If $D_{q+1}$ $[D_{q-1}]$ is divisible by the odd number $q$, $q$ being prime to $(\alpha - \beta)^2$, but $D_k$ is not divisible by $q$ for any factor $k$ of $q + 1$ $[q - 1]$, then $q$ is a prime number.*

From the easily verified relation

$$S_n^2 - (\alpha - \beta)^2 D_n^2 = 4\alpha^n \beta^n$$

and the fact that $D_n$ and $S_n$ are prime to $\alpha\beta$ it follows that $D_n$ and $S_n$ have no common odd prime factor. But

$$D_{2^k} = S_{2^{k-1}} D_{2^{k-1}} = S_{2^{k-1}} S_{2^{k-2}} \cdots S_{2^2} S_2 S_1.$$

Hence no two numbers in the sequence

$$S_{2^0},\ S_{2^1},\ S_{2^2},\ S_{2^3},\ \cdots$$

have a common odd prime factor.

11. For the application of these results to Fermat numbers $F_n$ let us take $\alpha + \beta = 2$, $\alpha\beta = -1$. Then $(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = 8$, a quadratic residue of a prime number $F_n$, since 2 is a quadratic residue of all primes of the form $8t + 1$. All the divisors of $F_n - 1$ are powers of 2. Moreover

$$D_{2^k} = S_{2^{k-1}} S_{2^{k-2}} \cdots S_2 S_1.$$

Hence we are concerned primarily with the numbers $G_1 = 6$, $G_2$, $G_3$, $\cdots$, where

$$G_s = S_{2^s}.$$

It is easy to verify directly the recurrence relation

$$G_{s+1} = G_s^2 - 2, \qquad s > 0.$$

Moreover no two $G$'s have a common odd prime factor, as we see from the statement at the close of § 10.

From the first theorem of the preceding section it follows that $D_{F_n - 1}$ is divisible by $F_n$ if $F_n$ is prime. Hence $F_n$ is composite if it divides no one of the numbers $G_1, G_2, \cdots G_{2^n - 1}$.

Suppose that $F_n$ divides $G_t$, $t < 2^n$, but no $G$ with subscript less than $t$. Then any prime factor $p$ of $F_n$ divides $G_t$ but no $G$ with subscript less than $t$, since the $G$'s are relatively prime in pairs. Hence $p$ is a factor of $D_{2^{t+1}}$ but of no

$D_s$ where $s < 2^{t+1}$. Hence $p$ is of the form $2^{t+1} \cdot q + 1$. Hence it follows that $F_n$ is prime if $2^{n-1} \leqq t \leqq 2^n - 1$; for, if $F_n$ is not prime, we should have

$$F_n = (2^{t+1} \cdot q_1 + 1)(2^{t+1} \cdot q_2 + 1) > 2^{2(t+1)} + 1;$$

or $2(t + 1) < 2^n$.

These results yield us the following remarkable theorem of Lucas:

*Consider the sequence* $G_1 = 6$, $G_2 = 34$, $G_3 = 1154$, $G_4, \cdots, G_{2^{n-1}}$, *each term of which is* 2 *less than the square of the preceding. Then* $F_n$ *is composite if it is a factor of no number of this sequence; if the first number of the sequence which* $F_n$ *divides is* $G_t$, *then every prime factor of* $F_n$ *is of the form* $2^{t+1} \cdot q + 1$, *and* $F_n$ *is a prime of this form if* $t \geqq 2^{n-1}$.

## Other Known Properties of the Numbers $F_n$.

12. A few other properties of the numbers $F_n$ should be mentioned.[1]

J. Hermes indicated a test for composite $F_n$ different from those given in the foregoing sections.

H. Scheffler noted that

$$F_n F_{n+1} \cdots F_{a-1} = 1 + 2^{2^n} + 2^{2 \cdot 2^n} + 2^{3 \cdot 2^n} + \cdots + 2^{2^a - 2^n}.$$

A. Cunningham considered the period of $1/N$ to base 2, where $N = F_m F_{m-1} \cdots F_{m-r}$. He noted that every $F_n > 5$ can be represented by four quadratic forms of determinants $\pm G_n$, $\pm 2G_n$, where $G_n = F_0 F_1 \cdots F_{n-1}$.

Gosset gave the complex prime factors $a \pm b\sqrt{-1}$ of the known real prime factors of composite $F_n$ for $n = 5, 6, 9, 11, 12, 18, 23, 36, 38$.

Cunningham gave several algebraic properties of the numbers $F_n$ (listed by Dickson at references 53, 55 and 56).

It is believed that all the essential known properties of the numbers $F_n$ are stated or referred to explicitly in the foregoing portions of this paper.

## Conjectures and Outstanding Problems Mentioned in the Literature.

13. Lucas[2] has listed five important problems in the theory of prime numbers, arranged in the "probable order of difficulty": (1) To find a prime greater than a given prime; (2) To find a function which yields only prime numbers; (3) To find the prime which follows a given prime; (4) To find the number of primes below a given limit; (5) To calculate directly the prime number of given rank. The first two of these would be simultaneously solved if one could prove the following conjecture:

All the numbers of the sequence

$$2^2 + 1, \quad 2^{2^2} + 1, \quad 2^{2^{2^2}} + 1, \quad \cdots$$

are primes. (The prime $2^8 + 1$ does not belong to this sequence.)

[1] See Dickson, *loc. cit.*, for references.

[2] *Théorie des nombres*, I, p. 354.

A proof of the foregoing conjecture would also carry with it the establishment of a theorem stated by Eisenstein, namely, that there is an infinitude of primes $F_n$. No proof of this theorem has yet been given.

Lipschitz[1] separated all integers into classes, the primes of one class being Fermat numbers, and gave a new interest to the question of the infinitude of primes $F_n$.

## Minor Additional Results.

14. Let $p$ be a prime proper factor of $F_n$ and write

$$p = 2^t \cdot k + 1$$

where $k$ may or may not contain the factor 2 but is not a power of 2. A proper prime factor of $F_n$ we shall call a Fermat prime factor.

Let us consider first the case in which $t = 2^\alpha$. (It is clear that $2^\alpha$ may, if desired, be taken not less than the highest power of 2 not exceeding $n + 2$.) From the congruences

$$2^{2^n} \equiv -1, \qquad 2^{2^\alpha} \cdot k \equiv -1 \bmod p$$

it is clear that we have

$$k^{2^{n-\alpha}} + 1 \equiv 0 \bmod p. \tag{1}$$

From this we have readily the following theorem:

*Every Fermat prime factor $p$ has the property that it is a factor of a number of the form*

$$a^{2^s} + 1$$

*in which $a$ is a factor of $p - 1$ belonging modulo $p$ to the exponent $2^{s+1}$ and is not a power of 2.*

The exponent $s$ need not be taken greater than $n - \alpha$ where $p$ is a factor of $F_n$ and $2^\alpha \leqq n - 2$.

For the case of the prime factor $p$, $p = 2^{2^\alpha} \cdot k + 1$, of $F_n$ it is obvious that $\alpha \leqq n - 1$. Consider the possibility that $\alpha = n - 1$. Then from (1) it follows that $k^2 + 1$ is divisible by $p$ and hence that $k > 2^{2^{n-1}}$; whence we have a contradiction. Therefore, $\alpha \leqq n - 2$.

We have $k^4 + 1$ divisible by $p$ when $\alpha = n - 2$; in view of (1) it is clear that it cannot be divisible by $p$ when $\alpha < n - 2$. Hence the Fermat prime factors $p$ of the form

$$p = 2^{2^{n-2}} \cdot k + 1$$

are all divisors of $k^4 + 1$ and no other Fermat prime factor $2^{2^\alpha} \cdot k + 1$ is a divisor of $k^4 + 1$.

In general, the Fermat prime factors of the form

$$2^{2^{n-v}} \cdot k + 1$$

[1] *Journ. für Math.*, 105, 152–156.

are divisors of $k^{2^v} + 1$ and no other Fermat prime factor $2^{2^a} \cdot k + 1$ is a divisor of $k^{2^v} + 1$.

15. In the Fermat prime factor $p$ of $F_n$,

$$p = 2^t \cdot k + 1,$$

let $t$ be an odd number. Then integers $r$ and $s$ exist such that

$$r \cdot 2^n - s \cdot t = 1.$$

From the congruences

$$2^{2^n} \equiv -1, \qquad 2^t \cdot k \equiv -1 \bmod p \tag{2}$$

we have

$$2^{r \cdot 2^n} \equiv (-1)^r, \qquad 2^{st} \cdot k^s \equiv (-1)^s \bmod p.$$

Hence we have

$$k^s \equiv (-1)^{r+s} \cdot 2 \bmod p.$$

It is clear that $s$ is odd. Hence we have

$$k^s \equiv (-1)^{r+1} \cdot 2 \bmod p. \tag{3}$$

Similarly, integers $r_1$ and $s_1$ exist such that

$$s_1 t - r_1 2^n = 1,$$

and we have readily

$$2k^s \equiv (-1)^{r_1+1} \bmod p. \tag{4}$$

If we multiply (3) through by 2 and compare the result with (4) we see that

$$k^{s-s_1} \equiv (-1)^{r+r_1} \cdot 4 \qquad \text{or} \qquad 4k^{s_1-s} \equiv (-1)^{r+r_1} \bmod p \tag{5}$$

according as $s > s_1$ or $s < s_1$.

Again, from (2) we have immediately that

$$k^{2^n} + 1 \equiv 0 \bmod p \tag{6}$$

so that $2^{2^n} + 1$ and $k^{2^n} + 1$ have the common factor $p$.

From the two equations

$$r2^n - st = 1, \qquad s_1 t - r_1 2^n = 1 \tag{7}$$

we see that

$$2^n(r + r_1) = t(s + s_1). \tag{8}$$

If $r, s$; $r_1, s_1$ are the least positive integers satisfying (7) it is clear that $s$ and $s_1$ are both less than $2^n$. Hence from (8) we see that

$$s + s_1 = 2^n, \qquad r + r_1 = t. \tag{9}$$

Then equations (5) are respectively

$$k^{s-s_1} + 4 \equiv 0, \qquad 4k^{s_1-s} + 1 \equiv 0 \bmod p, \tag{10}$$

16. By means of (1) and the known factorizations of $F_n$ one may readily obtain one numerical factor each of several binomial expressions. These are

given in the following table which contains in its first column a number $F_n$, in its second column a prime factor of $F_n$ and in its third column a binomial number having the same factor, the table being complete as to all known prime factors of composite $F_n$:

| | | |
|---|---|---|
| $F_5$ | $2^7 \cdot 5 + 1$ | $40^8 + 1$ |
| $F_5$ | $2^7 \cdot 52347 + 1$ | $418776^8 + 1$ |
| $F_6$ | $2^8 \cdot 3^2 \cdot 7 \cdot 17 + 1$ | $1071^8 + 1$ |
| $F_6$ | $2^8 \cdot 5 \cdot 52562829149 + 1$ | $262814145745^8 + 1$ |
| $F_9$ | $2^{16} \cdot 37 + 1$ | $37^{32} + 1$ |
| $F_{11}$ | $2^{13} \cdot 3 \cdot 13 + 1$ | $1248^{256} + 1$ |
| $F_{11}$ | $2^{13} \cdot 7 \cdot 17 + 1$ | $3808^{256} + 1$ |
| $F_{12}$ | $2^{14} \cdot 7 + 1$ | $448^{512} + 1$ |
| $F_{12}$ | $2^{16} \cdot 397 + 1$ | $397^{256} + 1$ |
| $F_{12}$ | $2^{16} \cdot 7 \cdot 139 + 1$ | $973^{256} + 1$ |
| $F_{18}$ | $2^{20} \cdot 13 + 1$ | $208^{2^{14}} + 1$ |
| $F_{23}$ | $2^{25} \cdot 5 + 1$ | $2560^{2^{19}} + 1$ |
| $F_{36}$ | $2^{39} \cdot 5 + 1$ | $640^{2^{31}} + 1$ |
| $F_{38}$ | $2^{41} \cdot 3 + 1$ | $1536^{2^{33}} + 1$ |
| $F_{73}$ | $2^{75} \cdot 5 + 1$ | $10240^{2^{67}} + 1$ |

In addition to the information furnished by these fifteen Fermat prime factors it is known that $F_0$, $F_1$, $F_2$, $F_3$, $F_4$ are prime and that $F_7$ and $F_8$ are composite, as we have said above.

17. In a similar way (3), (4) and (10) yield factors of other simple binomial expressions. We shall merely illustrate this by means of two examples involving (3). Taking the first factor $2^7 \cdot 5 + 1$ of $F_5$ we have $2 \cdot 32 - 9 \cdot 7 = 1$. Hence $s = 9$, $r = 2$. Therefore

$$5^9 + 2 \equiv 0 \bmod 2^7 \cdot 5 + 1.$$

Again, taking $n = 9$ we may write the given factor in the form $2^{15} \cdot 74 + 1$. Then we have $8 \cdot 512 - 273 \cdot 15 = 1$; whence

$$74^{273} + 2 \equiv 0 \bmod 2^{16} \cdot 37 + 1.$$

---

## SOME GEOMETRICAL RELATIONS OF THE PLANE, SPHERE, AND TETRAHEDRON.

By PHILIP FRANKLIN, College of the City of New York.

Professor Chrystal has remarked that mathematical works should be read backwards as well as forwards, *i. e.*, advanced notions of mathematics often throw light on elementary problems. While this "back tracking" is frequently brought out in analysis, it is seldom emphasized in connection with plane and solid geometry.